IN THE CLAIMS

There are no amendments to the claims.

1   1.   (Cancelled)

1   2.   (Cancelled)

1   3.   (Cancelled)

1   4.   (Cancelled)

1   5.   (Previously Presented) A computer-implemented system for protecting a
2 network, comprising:
3   a vulnerability detection system (VDS) for gathering information about the
4   network to determine vulnerabilities of a plurality of hosts on the
5   network; and
6   an intrusion detection system (IDS) for examining network traffic responsive
7   to the vulnerabilities of a host from the plurality of hosts as determined
8   by the VDS to detect traffic indicative of malicious activity.

1   6.   (Previously Presented) The system of claim 5, wherein the VDS is
2 adapted to gather information about the network by sending data to the plurality of hosts
3 and receiving responsive data from the plurality of hosts.

1   7.   (Previously Presented) The system of claim 5, wherein the VDS is
2 adapted to gather information automatically provided by the plurality of hosts.

1   8.   (Previously Presented) The system of claim 5, further comprising:
2   a vulnerabilities rules database, in communication with the VDS, for storing
3   rules describing vulnerabilities of the plurality of hosts,
4   wherein the VDS is adapted to analyze the gathered information with the rules
5   to determine the vulnerabilities of the plurality of hosts.

1   9.   (Previously Presented) The system of claim 8, wherein the VDS is
2   adapted to analyze the gathered information with the rules to identify operating systems
3   on the plurality of hosts and determine the vulnerabilities responsive to the respective
4   operating systems.

1   10.   (Previously Presented) The system of claim 8, wherein the VDS is
2   adapted to analyze the gathered information with the rules to identify open ports on the
3   plurality of hosts and determine the vulnerabilities based on the open ports.

1   11.   (Previously Presented) The system of claim 8, wherein the VDS is
2   adapted to analyze the gathered information with the rules to identify applications
3   executing on the plurality of hosts and determine the vulnerabilities based on the
4   applications.

1   12.   (Original) The system of claim 5, further comprising:
2   an intrusion rules database, in communication with the IDS, for storing rules
3   describing malicious activity,
4   wherein the IDS is adapted to analyze the network traffic with the rules to
5   detect network traffic indicative of exploitations of the determined
6   vulnerabilities.

1   13.   (Original) The system of claim 5, wherein the IDS is adapted to detect
2   traffic indicative of exploitations of only the determined vulnerabilities.

1   14.   (Cancelled)

1   15.   (Original) The system of claim 5, wherein the VDS is adapted to update
2   the determined vulnerabilities, and wherein the IDS is adapted to detect traffic indicative
3   of malicious activity in response to the update.

1   16.   (Original) The system of claim 15, wherein the VDS is adapted to update

2   the determined vulnerabilities in response to a change in the network.

1   17.   (Previously Presented) A computer-implemented method for protecting a

2   network, comprising:

3   gathering information about the network to determine vulnerabilities of a

4   plurality of hosts on the network; and

5   examining network traffic responsive to the determined vulnerabilities of a

6   host from the plurality of hosts to detect network traffic indicative of

7   malicious activity.

1   18.   (Previously Presented) The method of claim 17, wherein gathering

2   information comprises sending data to plurality of hosts on the network and receiving

3   responsive data from the plurality of hosts.

1   19.   (Previously Presented) The method of claim 17, wherein gathering

2   information comprises receiving data automatically provided by the plurality of hosts on

3   the network.

1   20.   (Previously Presented) The method of claim 17, further comprising:

2   storing rules to describe vulnerabilities of the plurality of hosts,

3   wherein determining vulnerabilities includes analyzing the gathered

4   information with the rules.

1   21.   (Previously Presented) The method of claim 20, wherein determining

2   vulnerabilities comprises analyzing the gathered information with the rules to identify

3   operating systems on the plurality of hosts.

1   22.   (Previously Presented) The method of claim 20, wherein determining

2   vulnerabilities comprises analyzing the gathered information with the rules to identify

3   open ports on the plurality of hosts.

1   23.   (Previously Presented) The method of claim 20, wherein determining

2 vulnerabilities comprises comparing the gathered information against the rules to identify

3 applications on the plurality of hosts.

1   24.   (Original) The method of claim 17, further comprising:

2   storing rules describing malicious activity,

3   wherein detecting network traffic indicative of malicious activity comprises

4   analyzing the network traffic with the rules to detect traffic indicative

5   of exploitations of the determined vulnerabilities.

1   25.   (Original) The method of claim 17, wherein examining network traffic

2 consists of detecting traffic indicative of exploitations of only the determined

3 vulnerabilities.

1   26.   (Cancelled)

1   27.   (Previously Presented) The method of claim 17, further comprising:

2   updating the determined vulnerabilities and detecting traffic indicative of

3   malicious activity in response to the update.

1   28.   (Original) The method of claim 27, wherein the updating is responsive to a

2 change in the network.

1   29.   (Previously Presented) A computer program product, comprising:

2   a computer-readable medium having computer program logic embodied

3   therein for protecting a network, the computer program logic:

4   gathering information about the network to determine vulnerabilities of a

5   plurality of hosts on the network; and

6   examining network traffic responsive to the determined vulnerabilities of a

7   host from the plurality of hosts to detect network traffic indicative of

8   malicious activity.

1   30.   (Previously Presented) The computer program product of claim 29,
2 wherein gathering information comprises sending data to plurality of hosts on the
3 network and receiving responsive data from the plurality of hosts.

1   31.   (Previously Presented) The computer program product of claim 29,
2 wherein gathering information comprises receiving data automatically provided by the
3 plurality of hosts on the network.

1   32.   (Previously Presented) The computer program product of claim 29,
2 further comprising:
3   storing rules to describe vulnerabilities of the plurality of hosts,
4   wherein determining vulnerabilities includes analyzing the gathered
5   information with the rules.

1   33.   (Previously Presented) The computer program product of claim 32,
2 wherein determining vulnerabilities comprises analyzing the gathered information with
3 the rules to identify operating systems on the plurality of hosts.

1   34.   (Previously Presented) The computer program product of claim 32,
2 wherein determining vulnerabilities comprises analyzing the gathered information with
3 the rules to identify open ports on the plurality of hosts.

1   35.   (Previously Presented) The computer program product of claim 32,
2 wherein determining vulnerabilities comprises comparing the gathered information
3 against the rules to identify applications on the plurality of hosts.

1   36.   (Original) The computer program product of claim 29, further comprising:
2   storing rules describing malicious activity,
3   wherein detecting network traffic indicative of malicious activity comprises
4   analyzing the network traffic with the rules to detect traffic indicative
5   of exploitations of the determined vulnerabilities.

1   37.   (Original) The computer program product of claim 29, wherein examining

2   network traffic consists of detecting traffic indicative of exploitations of only the verified

3   vulnerabilities.

1   38.   (Cancelled)

1   39.   (Previously Presented) The computer program product of claim 29, further

2   comprising:

3   updating the determined vulnerabilities; and

4   detecting traffic indicative of malicious activity in response to the update.

1   40.   (Previously Presented) The computer program product of claim 39,

2   wherein the updating is responsive to a change in the network.